The complexity of knapsack problems in wreath products

Michael Figelius
Universität Siegen, Germany

Moses Ganardi
Universität Siegen, Germany

Markus Lohrey
Universität Siegen, Germany

Georg Zetzsche
Max Planck Institute for Software Systems (MPI-SWS), Germany

Abstract

We prove new complexity results for computational problems in certain wreath products of groups and (as an application) for free solvable groups. For a finitely generated group we study the so-called power word problem (does a given expression $u_1^{k_1} \dots u_d^{k_d}$, where $u_1, \dots, u_d$ are words over the group generators and $k_1, \dots, k_d$ are binary encoded integers, evaluate to the group identity?) and knapsack problem (does a given equation $u_1^{x_1} \dots u_d^{x_d} = v$, where $u_1, \dots, u_d, v$ are words over the group generators and $x_1, \dots, x_d$ are variables, have a solution in the natural numbers). We prove that the power word problem for wreath products of the form $G \wr \mathbb{Z}$ with G nilpotent and iterated wreath products of free abelian groups belongs to TC^0. As an application of the latter, the power word problem for free solvable groups is in TC^0. On the other hand we show that for wreath products $G \wr \mathbb{Z}$, where G is a so called uniformly strongly efficiently non-solvable group (which form a large subclass of non-solvable groups), the power word problem is coNP-hard. For the knapsack problem we show NP-completeness for iterated wreath products of free abelian groups and hence free solvable groups. Moreover, the knapsack problem for every wreath product $G \wr \mathbb{Z}$, where G is uniformly efficiently non-solvable, is Σ_2^p-hard.

2012 ACM Subject Classification CCS → Theory of computation → computational complexity and cryptography → problems, reductions and completeness

Keywords and phrases algorithmic group theory, knapsack, wreath product

Digital Object Identifier 10.4230/LIPIcs.ICALP.2020.126

Related Version A full version of the paper is available at `https://arxiv.org/abs/2002.08086` [9].

Funding *Michael Figelius*: Funded by DFG project LO 748/12-1.
Markus Lohrey: Funded by DFG project LO 748/12-1.

1 Introduction

Since the seminal work of Dehn [7] on the word and conjugacy problem in surface groups, the area of combinatorial group theory [31] is tightly connected to algorithmic questions. The famous Novikov-Boone result [4, 40] on the existence of finitely presented groups with undecidable word problem was one of the first undecidability results that touched real mathematics. Since this pioneering work, the area of algorithmic group theory has been extended in many different directions. More general algorithmic problems have been studied and also the computational complexity of group theoretic problems has been investigated. In this paper, we focus on the decidability/complexity of two specific problems in group theory that have received considerable attention in recent years: the knapsack problem and the power word problem.

Knapsack problems There exist several variants of the classical knapsack problem over the integers [21]. In the variant that is particularly relevant for this paper, it is asked whether a linear equation $x_1 \cdot a_1 + \cdots + x_d \cdot a_d = b$, with $a_1, \ldots, a_d, b \in \mathbb{Z}$, has a solution $(x_1, \ldots, x_d) \in \mathbb{N}^d$. A proof for the NP-completeness of this problem for binary encoded integers $a_1, \ldots, a_d, b$ can be found in [15]. In contrast, if the numbers a_i, b are given in unary notation then the problem falls down into the circuit complexity class TC^0 [8]. In the course of a systematic investigation of classical commutative discrete optimization problems in non-commutative group theory, Myasnikov, Nikolaev, and Ushakov [33] generalized the above definition of knapsack to any f.g. group G: The input for the knapsack problem for G ($\mathrm{KP}(G)$ for short) is an equation of the form $g_1^{x_1} \cdots g_d^{x_d} = h$ for group elements $g_1, \ldots, g_d, h \in G$ (specified by finite words over the generators of G) and pairwise different variables $x_1, \ldots, x_d$ that take values in $\mathbb{N}$ and it is asked whether this equation has a solution (in Section 3.2, we formulate this problem in a slightly more general but equivalent way). In this form, $\mathrm{KP}(\mathbb{Z})$ is exactly the above knapsack problem for unary encoded integers studied in [8] (a unary encoded integer can be viewed as a word over a generating set $\{t, t^{-1}\}$ of $\mathbb{Z}$). For the case where $g_1, \ldots, g_d, h$ are commuting matrices over an algebraic number field, the knapsack problem has been studied in [1]. Let us emphasize that we are looking for solutions of knapsack equations in the natural numbers. One might also consider the variant, where the variables $x_1, \ldots, x_d$ take values in $\mathbb{Z}$. This latter version can be easily reduced to our knapsack version (with solutions in $\mathbb{N}$), but we are not aware of a reduction in the opposite direction.[1] Let us also mention that the knapsack problem is a special case of the more general rational subset membership problem [26].

We also consider a generalization of $\mathrm{KP}(G)$: An exponent equation is an equation of the form $g_1^{x_1} \cdots g_d^{x_d} = h$ as in the specification of $\mathrm{KP}(G)$, except that the variables $x_1, \ldots, x_d$ are not required to be pairwise different. *Solvability of exponent equations* for G ($\textsc{ExpEq}(G)$ for short) is the problem where the input is a conjunction of exponent equations (possibly with shared variables) and the question is whether there is a joint solution for these equations in the natural numbers.

Let us briefly survey the results about knapsack obtained in [33] and subsequent papers:

- Knapsack can be solved in polynomial time for every hyperbolic group [33]. Some extensions of this result can be found in [11, 25].

[1] Note that the problem whether a given system of linear equations has a solution in $\mathbb{N}$ is NP-complete, whereas the problem can be solved in polynomial time (using the Smith normal form) if we ask for a solution in $\mathbb{Z}$. In other words, if we consider the knapsack problem for $\mathbb{Z}^n$ with n part of the input, then looking for solutions in $\mathbb{N}$ seems to be more difficult than looking for solutions in $\mathbb{Z}$.

- There are nilpotent groups of class 2 for which knapsack is undecidable. Examples are direct products of sufficiently many copies of the discrete Heisenberg group $H_3(\mathbb{Z})$ [22], and free nilpotent groups of class 2 and sufficiently high rank [37]. In contrast, knapsack for $H_3(\mathbb{Z})$ is decidable [22]. Thus, direct products to not preserve decidability of knapsack.
- Knapsack is decidable for every co-context-free group [22], i.e., groups where the set of all words over the generators that do not represent the identity is a context-free language. Lehnert and Schweitzer [23] have shown that the Higman-Thompson groups are co-context-free.
- Knapsack belongs to NP for all virtually special groups (finite extensions of subgroups of graph groups) [28]. The class of virtually special groups is very rich. It contains all Coxeter groups, one-relator groups with torsion, fully residually free groups, and fundamental groups of hyperbolic 3-manifolds. For graph groups (a.k.a. right-angled Artin groups) a complete classification of the complexity was obtained in [29]: If the underlying graph contains an induced path or cycle on 4 nodes, then knapsack is NP-complete; in all other cases knapsack can be solved in polynomial time (even in LogCFL).
- Knapsack is NP-complete for every wreath product $A \wr \mathbb{Z}$ with $A \neq 1$ f.g. abelian [12] (wreath products are formally defined in Section 3.1).
- Decidability of knapsack is preserved under finite extensions, HNN-extensions over finite associated subgroups and amalgamated free products over finite subgroups [28].

For a knapsack equation $g_1^{x_1} \cdots g_d^{x_d} = h$ we may consider the set of all solutions $\{(n_1, \ldots, n_d) \in \mathbb{N}^d \mid g_1^{n_1} \cdots g_d^{n_d} = g \text{ in } G\}$. In the papers [25, 22, 29] it turned out that in many groups the solution set of every knapsack equation is a *semilinear set* (see Section 2 for a definition). We say that a group is *knapsack-semilinear* if for every knapsack equation the set of all solutions is semilinear and a semilinear representation can be computed effectively (the same holds then also for exponent equations). Note that in any group G the set of solutions on an equation $g^x = h$ is periodic and hence semilinear. This result generalizes to solution sets of knapsack instances of the for $g_1^x g_2^y = h$ (see Lemma 9), but there are examples of knapsack instances with three variables where solutions sets (in certain groups) are not semilinear. Examples of knapsack-semilinear groups are graph groups [29] (which include free groups and free abelian groups), hyperbolic groups [25], and co-context free groups [22].[2] Moreover, the class of knapsack-semilinear groups is closed under finite extensions, graph products, amalgamated free products with finite amalgamated subgroups, HNN-extensions with finite associated subgroups (see [10] for these closure properties) and wreath products [12].

Power word problems In the power word problem for a f.g. group G ($\textsc{PowerWP}(G)$ for short) the input consists of an expression $u_1^{n_1} u_2^{n_2} \cdots u_d^{n_d}$, where $u_1, \ldots, u_d$ are words over the group generators and $n_1, \ldots, n_d$ are binary encoded integers. The problem is then to decide whether the expression $u_1^{n_1} u_2^{n_2} \cdots u_d^{n_d}$ evaluates to the identity in G. The power word problem arises very naturally in the context of the knapsack problem: it allows us to verify a proposed solution for a knapsack equation with binary encoded numbers. The power word problem has been first studied in [27], where it was shown that the power word problem for f.g. free groups has the same complexity as the word problem and hence can be solved in logarithmic space. Other groups with easy power word problems are f.g. nilpotent groups and wreath products $A \wr \mathbb{Z}$ with A f.g. abelian [27]. In contrast it is shown in [27] that the power word problem for wreath products $G \wr \mathbb{Z}$, where G is either finite non-solvable

[2] Knapsack-semilinearity of co-context free groups is not stated in [22] but follows immediately from the proof for the decidability of knapsack.

or f.g. free, is coNP-complete. Implicitly, the power word problem appeared also in the work of Ge [13], where it was shown that one can verify in polynomial time an identity $\alpha_1^{n_1}\alpha_2^{n_2}\cdots\alpha_d^{n_d}=1$, where the α_i are elements of an algebraic number field and the n_i are binary encoded integers. The power word problem is a special case of the compressed word problem [24], which asks whether a grammar-compressed word over the group generators evaluates to the group identity.

Main results Our main focus is on the problems $\textsc{PowerWP}(G)$, $\mathrm{KP}(G)$ and $\textsc{ExpEq}(G)$ for the case where G is a wreath product. We start with the following result:

▶ **Theorem 1.** *$\textsc{PowerWP}(G \wr \mathbb{Z})$ is in TC^0 for every f.g. nilpotent group G.*

Theorem 1 generalizes the above mentioned result from [27] (for G abelian) in a nontrivial way. Our proof analyzes periodic infinite words over a nilpotent group G. Roughly speaking, we show that one can check in TC^0, whether a given list of such periodic infinite words pointwise multiplies to the identity of G. We believe that this is a result of independent interest. We use this result also in the proof of the following theorem:

▶ **Theorem 2.** *$\mathrm{KP}(G \wr \mathbb{Z})$ is NP-complete for every finite nilpotent group $G \neq 1$.*

Next, we consider iterated wreath products. Fix $r \geq 1$ and define the iterated wreath products $W_{0,r} = \mathbb{Z}^r$ and $W_{m+1,r} = \mathbb{Z}^r \wr W_{m,r}$. By a famous result of Magnus [32] the free solvable group $S_{m,r}$ of derived length r and rank m embeds into $W_{m,r}$. Our main results for these groups are:

▶ **Theorem 3.** *$\textsc{PowerWP}(W_{m,r})$ and hence $\textsc{PowerWP}(S_{m,r})$ is in TC^0 for $m \geq 0$, $r \geq 1$.*

It was only recently shown in [35] that the word problem (and the conjugacy problem) for every free solvable group belongs to TC^0. Theorem 3 generalizes TC^0 membership of the word problem.

▶ **Theorem 4.** *$\textsc{ExpEq}(W_{m,r})$ and hence $\textsc{ExpEq}(S_{m,r})$ is NP-complete for $m \geq 0$, $r \geq 1$.*

For the proof of Theorem 4 we show that if a given knapsack equation over $W_{m,r}$ has a solution then it has a solution where all numbers are exponentially bounded in the length of the knapsack instance. Theorem 4 then follows easily from Theorem 3. For some other algorithmic results for free solvable groups see [34].

Finally, we show new hardness results for the power word problem and knapsack problem. For this we make use so-called *uniformly strongly efficiently non-solvable* groups (uniformly SENS groups) that were recently defined in [3]. Roughly speaking, a group G is uniformly SENS if there exists nontrivial nested commutators of arbitrary depth that moreover, are efficiently computable in a certain sense (see Section 6 for the precise definition). The essence of these groups is that they allow to carry out Barrington's argument showing the NC^1-hardness of the word problem for a finite solvable group [2]. We prove the following:

▶ **Theorem 5.** *$\textsc{PowerWP}(G \wr \mathbb{Z})$ is coNP-hard for every f.g. uniformly SENS group G.*

This result generalizes a result from [27] saying that $\textsc{PowerWP}(G \wr \mathbb{Z})$ is coNP-hard for the case that G is f.g. free or finite non-solvable.

▶ **Theorem 6.** *$\mathrm{KP}(G \wr \mathbb{Z})$ is Σ_2^p-hard for every f.g. uniformly SENS group G.*

Recall that for every nontrivial group G, $\mathrm{KP}(G \wr \mathbb{Z})$ is NP-hard [12]. We also show several corollaries of Theorems 5 and 6. For instance, we show that for the famous Thompson's group F, $\textsc{PowerWP}(F)$ is coNP-complete and $\mathrm{KP}(F)$ is Σ_2^p-hard.

2 Preliminaries

Complexity theory We assume some knowledge in complexity theory; in particular the reader should be familiar with the classes P, NP, and coNP. The class Σ_2^p (second existential level of the polynomial time hierarchy) contains all languages $L \subseteq \Sigma^*$ for which there exists a polynomial p and a language $K \subseteq \Sigma^*\#\{0,1\}^*\#\{0,1\}^*$ in P (for a symbol $\# \notin \Sigma \cup \{0,1\}$) such that $x \in L$ if and only if $\exists y \in \{0,1\}^{\leq p(|x|)} \forall z \in \{0,1\}^{\leq p(|x|)} : x\#y\#z \in K$.

The class TC^0 contains all problems that can be solved by a family of threshold circuits of polynomial size and constant depth. In this paper, TC^0 will always refer to the $\mathsf{DLOGTIME}$-uniform version of TC^0. A precise definition is not needed for our work; see [42] for details. All we need is that the following arithmetic operations on binary encoded integers belong to TC^0: iterated addition and multiplication (i.e., addition and multiplication of n many n-bit numbers) and division with remainder.

For languages (or computational problems) $A, B_1, \ldots, B_k \subseteq \{0,1\}^*$ we write $A \in \mathsf{TC}^0(B_1, \ldots, B_k)$ (A is TC^0-Turing-reducible to $B_1, \ldots, B_k$) if A can be solved by a family of threshold circuits of polynomial size and constant depth that in addition may also use oracle gates for the languages $B_1, \ldots, B_k$ (an oracle gate for B_i yields the output 1 if and only if the string of input bits belongs to B_i).

Semilinear sets Fix a dimension $d \geq 1$. All vectors will be column vectors. For a vector $\boldsymbol{v} = (v_1, \ldots, v_d)^\mathsf{T} \in \mathbb{Z}^d$ we define its norm $\|\boldsymbol{v}\| := \max\{|v_i| \mid 1 \leq i \leq d\}$ and for a matrix $M \in \mathbb{Z}^{c \times d}$ with entries $m_{i,j}$ ($1 \leq i \leq c$, $1 \leq j \leq d$) we define the norm $\|M\| = \max\{|m_{i,j}| \mid 1 \leq i \leq c, 1 \leq j \leq d\}$. Finally, for a finite set of vectors $A \subseteq \mathbb{N}^d$ let $\|A\| = \max\{\|\boldsymbol{a}\| \mid \boldsymbol{a} \in A\}$. We extend the operations of vector addition and multiplication of a vector by a matrix to sets of vectors in the obvious way. A *linear subset* of $\mathbb{N}^d$ is a set of the form $L = L(\boldsymbol{b}, P) := \boldsymbol{b} + P \cdot \mathbb{N}^k$, where $\boldsymbol{b} \in \mathbb{N}^d$ and $P \in \mathbb{N}^{d \times k}$. A set $S \subseteq \mathbb{N}^d$ is called *semilinear* if it is a finite union of linear sets. Semilinear sets play an important role in automata theory, logic, and other areas. They are precisely the sets definable in Presburger arithmetic, i.e. first-order logic over the structure $(\mathbb{N}, +)$, and thus form a Boolean algebra.

For a semilinear set $S = \bigcup_{i=1}^k L(\boldsymbol{b}_i, P_i)$, we call the tuple $(\boldsymbol{b}_1, P_1, \ldots, \boldsymbol{b}_k, P_k)$ a *semilinear representation* of S. The magnitude of the semilinear representation $(\boldsymbol{b}_1, P_1, \ldots, \boldsymbol{b}_k, P_k)$ is $\max\{\|\boldsymbol{b}_1\|, \|P_1\| \ldots, \|\boldsymbol{b}_k\|, \|P_k\|\}$. The *magnitude* $\|S\|$ of a semilinear set S is the minimal magnitude of all semilinear representations for S.

It is often convenient to treat mappings $\nu \colon \{x_1, \ldots, x_d\} \to \mathbb{N}$, where $X = \{x_1, \ldots, x_d\}$ is a finite set of variables, as vectors. To this end, we identify ν with the vector $(\nu(x_1), \ldots, \nu(x_d))^\mathsf{T}$. This way, vector operations (e.g. addition and scalar multiplication) and the notion of semilinearity carry over to the set $\mathbb{N}^X$ of all mappings from X to $\mathbb{N}$.

3 Groups

We assume that the reader is familiar with the basics of group theory. Let G be a group. We always write 1 for the group identity element. For $g, h \in G$ we write $[g, h] := g^{-1}h^{-1}gh$ for the commutator of g and h and g^h for $h^{-1}gh$. For subgroups A, B of G we write $[A, B]$ for the subgroup generated by all commutators $[a, b]$ with $a \in A$ and $b \in B$. The order of an element $g \in G$ is the smallest number $z > 0$ with $g^z = 1$ and ∞ if such a z does not exist. The group G is torsion-free, if every $g \in G \setminus \{1\}$ has infinite order.

We say that G is *finitely generated (f.g.)* if there is a finite subset $\Sigma \subseteq G$ such that every element of G can be written as a product of elements from Σ; such a Σ is called a *finite generating set* for G. We also write $G = \langle \Sigma \rangle$. We then have a canonical morphism $h\colon \Sigma^* \to G$ that maps a word over Σ to its product in G. If $h(w) = 1$ we also say that $w = 1$ in G. For $g \in G$ we write $|g|$ for the length of a shortest word $w \in \Sigma^*$ such that $h(w) = g$. This notation depends on the generating set Σ. We always assume that the generating set Σ is symmetric in the sense that $a \in \Sigma$ implies $a^{-1} \in \Sigma$. Then, we can define on Σ^* a natural involution $\cdot^{-1}$ by $(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} a_1^{-1}$ for $a_1, a_2, \dots, a_n \in \Sigma$. This allows to use the notations $[g, h] = g^{-1}h^{-1}gh$ and $g^h = h^{-1}gh$ in the case $g, h \in \Sigma^*$. By *computing a homomorphism* $h\colon G_1 = \langle \Sigma_1 \rangle \to G_2 = \langle \Sigma_2 \rangle$, we mean computing the images $h(a)$ for $a \in \Sigma_1$.

A group G is called *orderable* if there exists a linear order $\leq$ on G such that $g \leq h$ implies $xgy \leq xhy$ for all $g, h, x, y \in G$ [39, 38]. Every orderable group is torsion-free (this follows directly from the definition) and has the unique roots property [41], i.e., $g^n = h^n$ implies $g = h$. The are numerous examples of orderable groups: for instance, torsion-free nilpotent groups, right-angled Artin groups, and diagram groups are all orderable.

Two elements $g, h \in G$ in a group G are called *commensurable* if $g^x = h^y$ for some $x, y \in \mathbb{Z} \setminus \{0\}$. This defines an equivalence relation on G, in which the elements with finite order form an equivalence class. By [39, Corollary 1.2] commensurable elements in an orderable group commute.

3.1 Wreath products

Let G and H be groups. Consider the direct sum $K = \bigoplus_{h \in H} G_h$, where G_h is a copy of G. We view K as the set $G^{(H)}$ of all mappings $f\colon H \to G$ such that $\mathrm{supp}(f) := \{h \in H \mid f(h) \neq 1\}$ is finite, together with pointwise multiplication as the group operation. The set $\mathrm{supp}(f) \subseteq H$ is called the *support* of f. The group H has a natural left action on $G^{(H)}$ given by $hf(a) = f(h^{-1}a)$, where $f \in G^{(H)}$ and $h, a \in H$. The corresponding semidirect product $G^{(H)} \rtimes H$ is the (restricted) *wreath product* $G \wr H$. In other words:

- Elements of $G \wr H$ are pairs (f, h), where $h \in H$ and $f \in G^{(H)}$.
- The multiplication in $G \wr H$ is defined as follows: Let $(f_1, h_1), (f_2, h_2) \in G \wr H$. Then $(f_1, h_1)(f_2, h_2) = (f, h_1 h_2)$, where $f(a) = f_1(a) f_2(h_1^{-1} a)$.

There are canonical mappings

- $\sigma\colon G \wr H \to H$ with $\sigma(f, h) = h$ and
- $\tau\colon G \wr H \to G^{(H)}$ with $\tau(f, h) = f$

In other words: $g = (\tau(g), \sigma(g))$ for $g \in G \wr H$. Note that σ is a homomorphism whereas τ is in general not a homomorphism. Throughout this paper, the letters σ and τ will have the above meaning, which of course depends on the underlying wreath product $G \wr H$, but the latter will be always clear from the context.

The following intuition might be helpful: An element $(f, h) \in G \wr H$ can be thought of as a finite multiset of elements of $G \setminus \{1_G\}$ that are sitting at certain elements of H (the mapping f) together with the distinguished element $h \in H$, which can be thought of as a cursor moving in H. If we want to compute the product $(f_1, h_1)(f_2, h_2)$, we do this as follows: First, we shift the finite collection of G-elements that corresponds to the mapping f_2 by h_1: If the element $g \in G \setminus \{1_G\}$ is sitting at $a \in H$ (i.e., $f_2(a) = g$), then we remove g from a and put it to the new location $h_1 a \in H$. This new collection corresponds to the mapping $f_2'\colon a \mapsto f_2(h_1^{-1} a)$. After this shift, we multiply the two collections of G-elements pointwise: If in $a \in H$ the elements g_1 and g_2 are sitting (i.e., $f_1(a) = g_1$ and $f_2'(a) = g_2$), then we put the product $g_1 g_2$ into the location a. Finally, the new distinguished H-element (the new cursor position) becomes $h_1 h_2$.

Clearly, H is a subgroup of $G \wr H$. We also regard G as a subgroup of $G \wr H$ by identifying G with the set of all $f \in G^{(H)}$ with $\mathrm{supp}(f) \subseteq \{1\}$. This copy of G together with H generates

$G \wr H$. In particular, if $G = \langle \Sigma \rangle$ and $H = \langle \Gamma \rangle$ with $\Sigma \cap \Gamma = \emptyset$ then $G \wr H$ is generated by $\Sigma \cup \Gamma$. In this situation, we will also apply the above mappings σ and τ to words over $\Sigma \cup \Gamma$.

In [34] it was shown that the word problem of a wreath product $G \wr H$ is TC^0-reducible to the word problems for G and H. Let us briefly sketch the argument. Assume that $G = \langle \Sigma \rangle$ and $H = \langle \Gamma \rangle$. Given a word $w \in (\Sigma \cup \Gamma)^*$ one has to check whether $\sigma(w) = 1$ in H and $\tau(w)(h) = 1$ in H for all h in the support of $\tau(w)$. One can compute in TC^0 the word $\sigma(w)$ by projecting w onto the alphabet Γ. Moreover, one can enumerate the support of $\tau(w)$ by going over all prefixes of w and checking which σ-values are the same. Similarly, one produces for a given $h \in \mathrm{supp}(\tau(w))$ a word over Σ that represents $\tau(w)(h)$.

We will need the following result from [30] (which holds only for the so-called restricted wreath product that we consider in this paper):

▶ **Theorem 7** ([30]). *If G and H are orderable then also $G \wr H$ is orderable.*

3.2 Knapsack problem

Let $G = \langle \Sigma \rangle$ be a f.g. group. An *exponent expression* over G is an expression of the form $E = v_0 u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_d^{x_d} v_d$ with $d \geq 1$, words $v_0, \ldots, v_d \in \Sigma^*$, non-empty words $u_1, \ldots, u_d \in \Sigma^*$, and variables $x_1, \ldots, x_d$. Here, we allow $x_i = x_j$ for $i \neq j$. If every variable x_i occurs at most once, then E is called a *knapsack expression*. Let $X = \{x_1, \ldots, x_d\}$ be the set of variables that occur in E. For a homomorphism $h \colon G \to G' = \langle \Sigma' \rangle$ (that is specified by a mapping from Σ to $(\Sigma' \cup \Sigma'^{-1})^*$), we denote with $h(E)$ the exponent expression $h(v_0)h(u_1)^{x_1}h(v_1)h(u_2)^{x_2}h(v_2) \cdots h(u_d)^{x_d}h(v_d)$. For a mapping $\nu \in \mathbb{N}^X$, we define $\nu(E) = v_0 u_1^{\nu(x_1)} v_1 u_2^{\nu(x_2)} v_2 \cdots u_d^{\nu(x_d)} v_d \in \Sigma^*$. We say that ν is a *G-solution* for E if $\nu(E) = 1$ in G. With $\mathrm{sol}_G(E)$ we denote the set of all G-solutions of E. The *length* of E is defined as $|E| = \sum_{i=1}^{d} |u_i| + |v_i|$. We define *solvability of exponent equations over G*, $\textsc{ExpEq}(G)$ for short, as the following decision problem:

Input A finite list of exponent expressions $E_1, \ldots, E_n$ over G.

Question Is $\bigcap_{i=1}^{n} \mathrm{sol}_G(E_i)$ non-empty?

The *knapsack problem for G*, $\mathrm{KP}(G)$ for short, is the following decision problem:

Input A single knapsack expression E over G.

Question Is $\mathrm{sol}_G(E)$ non-empty?

It is an easy observation that the choice of the generating set Σ has no influence on the decidability or complexity of these problems. For the knapsack problem in wreath products the following result has been shown in [12]:

▶ **Theorem 8** ([12]). *For every nontrivial group G, $\mathrm{KP}(G \wr \mathbb{Z})$ is NP-hard.*

3.3 Knapsack-semilinear groups

The group G is called *knapsack-semilinear* if for every knapsack expression E over Σ, the set $\mathrm{sol}_G(E)$ is a semilinear set of vectors and a semilinear representation can be effectively computed from E. Since semilinear sets are effectively closed under intersection, it follows that for every exponent expression E over Σ, the set $\mathrm{sol}_G(E)$ is semilinear and a semilinear representation can be effectively computed from E. Moreover, solvability of exponent equations is decidable for every knapsack-semilinear group. As mentioned above, the class of knapsack-semilinear groups is very rich. An example of a group G, where knapsack is decidable but solvability of exponent equations is undecidable is the Heisenberg group $H_3(\mathbb{Z})$ (which consists of all upper triangular (3×3)-matrices over the integers, where all diagonal entries are 1), see [22]. In particular, $H_3(\mathbb{Z})$ is not knapsack-semilinear. A non-semilinear solution set can be achieved with a three-variable knapsack instance over $H_3(\mathbb{Z})$. For two variables, the solutions sets are semilinear for any group. In fact, they have a particularly simple structure:

▶ **Lemma 9.** *Let G be a group and $g_1, g_2, h \in G$ be elements.*

(i) *The solution set $S_1 = \{(x,y) \in \mathbb{Z}^2 \mid g_1^x g_2^y = 1\}$ is a subgroup of $\mathbb{Z}^2$. If G is torsion-free and $\{g_1, g_2\} \neq \{1\}$ then S_1 is cyclic.*

(ii) *The solution set $S = \{(x,y) \in \mathbb{Z}^2 \mid g_1^x g_2^y = h\}$ is either empty or a coset $(a,b) + S_1$ of S_1 where $(a,b) \in S$ is any solution.*

For a knapsack-semilinear group G and a finite generating set Σ for G we define a growth function. For $n \in \mathbb{N}$ let $\mathsf{Knap}(n)$ (resp., $\mathsf{Exp}(n)$) be the finite set of all knapsack expressions (resp., exponent expression) E over Σ such that $\mathrm{sol}_G(E) \neq \emptyset$ and $|E| \leq n$. We define the mapping $\mathsf{K}_{G,\Sigma} \colon \mathbb{N} \to \mathbb{N}$ and $\mathsf{E}_{G,\Sigma} \colon \mathbb{N} \to \mathbb{N}$ as follows:

$$\mathsf{K}_{G,\Sigma}(n) = \max\{\|\mathrm{sol}_G(E)\| \mid E \in \mathsf{Knap}(n)\}, \quad (1)$$

$$\mathsf{E}_{G,\Sigma}(n) = \max\{\|\mathrm{sol}_G(E)\| \mid E \in \mathsf{Exp}(n)\}. \quad (2)$$

Clearly, if $\mathrm{sol}_G(E) \neq \emptyset$ and $\|\mathrm{sol}_G(E)\| \leq N$ then E has a G-solution ν such that $\nu(x) \leq N$ for all variables x that occur in E. Thus, if G has a decidable word problem and a computable bound on the function $\mathsf{K}_{G,\Sigma}$, then we can solve $\mathrm{KP}(G)$ non-deterministically: given a knapsack expression E with variables from X, we guess $\nu \colon X \to \mathbb{N}$ with $\sigma(x) \leq N$ for all variables x and then check (using an algorithm for the word problem) whether ν is a solution.

Let Σ and Σ' be two generating sets for the group G. Then there is a constant c such that $\mathsf{K}_{G,\Sigma}(n) \leq \mathsf{K}_{G,\Sigma'}(cn)$, and similarly for $\mathsf{E}_{G,\Sigma}(n)$. To see this, note that for every $a \in \Sigma'$ there is a word $w_a \in \Sigma^*$ such that a and w_a represent the same element in G. Then we can choose $c = \max\{|w_a| \mid a \in \Sigma'\}$. Due to this fact, we do not have to specify the generating set Σ when we say that $\mathsf{K}_{G,\Sigma}$ (resp., $\mathsf{E}_{G,\Sigma}$) is polynomially/exponentially bounded.

Important for us is also the following result from [12]:

▶ **Theorem 10** ([12])**.** *If G and H are knapsack-semilinear then so is $G \wr H$.*

The proof of this result in [12] does not yield a good bound of $\mathsf{K}_{G \wr H}(n)$ in terms of $\mathsf{K}_G(n)$ and $\mathsf{K}_H(n)$ (and similarly for the E-function). One of our main achievements is such a bound for the case that the left factor G is f.g. abelian. For $\mathsf{E}_G(n)$ we then have the following bound, which follows from well-known bounds on solutions of linear Diophantine equations [43]:

▶ **Lemma 11.** *If G is a f.g. abelian group then $\mathsf{E}_G(n) \leq 2^{n^{\mathcal{O}(1)}}$.*

3.4 Power word problem

A *power word* (over Σ) is a tuple $(u_1, k_1, u_2, k_2, \ldots, u_d, k_d)$ where $u_1, \ldots, u_d \in \Sigma^*$ are words over the group generators (called the periods of the power word) and $k_1, \ldots, k_d \in \mathbb{Z}$ are integers that are given in binary notation. Such a power word represents the word $u_1^{k_1} u_2^{k_2} \cdots u_d^{k_d}$. We will often identify the power word $(u_1, k_1, u_2, k_2, \ldots, u_d, k_d)$ with the word $u_1^{k_1} u_2^{k_2} \cdots u_d^{k_d}$. Moreover, if $k_i = 1$, then we usually omit the exponent 1 in a power word. The *power word problem* for the f.g. group G, $\textsc{PowerWP}(G)$ for short, is the following:

Input A power word $(u_1, k_1, u_2, k_2, \ldots, u_d, k_d)$.

Question Does $u_1^{k_1} u_2^{k_2} \cdots u_d^{k_d} = 1$ hold in G?

Due to the binary encoded exponents, a power word can be seen as a succinct description of an ordinary word. We have the following simple lemma.

▶ **Lemma 12.** *If the f.g. group G is knapsack-semilinear, $\mathsf{E}_G(n)$ is exponentially bounded, and $\textsc{PowerWP}(G)$ belongs to NP then $\textsc{ExpEq}(G)$ belongs to NP.*

4 Wreath products of nilpotent groups and the integers

Nilpotent groups. The *lower central series* of a group G is the sequence of groups $(G_i)_{i\geq 0}$ with $G_0 = G$ and $G_{i+1} = [G_i, G]$. The group G is *nilpotent* if there is a $c \geq 0$ with $G_c = 1$; in this case the minimal c with $G_c = 1$ is called the *nilpotency class* of G. In this section we prove Theorems 1 and 2. Our main tool are periodic words over G as introduced in [12].

Periodic words over groups. Let $G = \langle \Sigma \rangle$ be a f.g. group. Let G^ω be the set of all functions $f\colon \mathbb{N} \to G$, which forms a group by pointwise multiplication $(fg)(t) = f(t) \cdot g(t)$. A function $f \in G^\omega$ is *periodic* if there exists a number $d \geq 1$ such that $f(t) = f(t + d)$ for all $t \geq 0$. The smallest such d is called the *period* of f. If $f \in G^\omega$ has period d and $g \in G^\omega$ has period e then fg has period at most $\mathrm{lcm}(d, e)$. A periodic function $f \in G^\omega$ with period d can be specified by its initial d elements $f(0), \dots, f(d - 1)$ where each element $f(t)$ is given as a word over the generating set Σ. The *periodic words problem* $\textsc{Periodic}(G)$ over G is the following:

Input Periodic functions $f_1, \dots, f_m \in G^\omega$ and a binary encoded number T.

Question Does the product $f = \prod_{i=1}^m f_i$ satisfy $f(t) = 1$ for all $t \leq T$?

We shall derive Theorems 1 and 2 from the following result:

▶ **Theorem 13.** *If G is a f.g. nilpotent group then $\textsc{Periodic}(G)$ belongs to TC^0.*

Previously it was proven that $\textsc{Periodic}(G)$ belongs to TC^0 if G is abelian [12]. As an introduction let us reprove this result.

Let $\rho\colon G^\omega \to G^\omega$ be the *shift*-operator, i.e. $(\rho(f))(t) = f(t + 1)$, which is a group homomorphism. For a subgroup H of G^ω, we denote by $H^{(n)}$ the smallest subgroup of G^ω that contains $\rho^0(H), \rho^1(H), \dots, \rho^n(H)$. Note that $(H^{(m)})^{(n)} = H^{(m+n)}$ for any $m, n \in \mathbb{N}$. A function $f \in G^\omega$ *satisfies a recurrence of order* $d \geq 1$ if $\rho^d(f)$ is contained in the subgroup $\langle f \rangle^{(d-1)}$ of G^ω. If f has period d then f clearly satisfies a recurrence of order d.

Let us now consider the case that G is abelian. Then, also G^ω is abelian and we use the additive notation for G^ω. The following lemma is folklore:

▶ **Lemma 14** (cf. [17]). *Let G be a f.g. abelian group. If $f_1, \dots, f_m \in G^\omega$ satisfy recurrences of order $d_1, \dots, d_m \geq 1$ respectively, then $\sum_{i=1}^m f_i$ satisfies a recurrence of order $\sum_{i=1}^m d_i$.*

Proof. Observe that G^ω is a $\mathbb{Z}[x]$-module with scalar multiplication

$$\sum_{i=0}^{d} a_i x^i \cdot f \mapsto \sum_{i=0}^{d} a_i \rho^i(f). \tag{3}$$

Then $f \in G^\omega$ satisfies a recurrence of order $d \geq 1$ if and only if there exists a monic polynomial $p \in \mathbb{Z}[x]$ of degree d (where monic means that the leading coefficient is one) such that $pf = 0$. Therefore, if $p_1, \dots, p_m \in \mathbb{Z}[x]$ such that $\deg(p_i) = d_i \geq 1$ and $p_i f_i = 0$ then $\prod_{i=1}^m p_i \sum_{j=1}^m f_j = \sum_{j=1}^m (\prod_{i=1}^m p_i) f_j = 0$. Since $\prod_{i=1}^m p_i$ is a monic polynomial of degree $d := \sum_{i=1}^m d_i$, $\sum_{i=1}^m f_i$ satisfies a recurrence of order d. ◀

The above lemma implies that $\sum_{i=1}^m f_i = 0$ if and only if $\sum_{i=1}^m f_i(t) = 0$ for all $0 \leq t \leq d - 1$, where d is the sum of the periods of the f_i.

Let us now turn to the nilpotent case. For $n \in \mathbb{N}$, let $G^{\omega,n}$ be the subgroup of G^ω generated by all elements with period at most n. Then $G^{\omega,n}$ is closed under shift. The key fact for showing Theorem 13 is the following.

▶ **Proposition 15.** *If G is a f.g. nilpotent group, then there is a polynomial p such that every element of $G^{\omega,n}$ satisfies a recurrence of order $p(n)$.*

Let $H \le G^\omega$ be a subgroup which is closed under shifting, i.e. $\rho(H) \subseteq H$. Since the shift is a homomorphism, the commutator subgroup $[H,H]$ is closed under shifting as well. We will work in the abelianization $H' = H/[H,H]$ where we write $\bar{f}$ for the coset $f[H,H]$. We also define $\rho\colon H' \to H'$ by $\rho(\bar{f}) = \overline{\rho(f)}$. This is well-defined since $fg^{-1} \in [H,H]$ implies $\rho(f)\rho(g)^{-1} = \rho(fg^{-1}) \in [H,H]$ and hence $\overline{\rho(f)} = \overline{\rho(g)}$. As an abelian group H' is a $\mathbb{Z}$-module and, in fact, H' forms a $\mathbb{Z}[x]$-module using the shift-operator. By the above remark (see (3)) we have the following (where we use the multiplicative notation for H'):

▶ **Lemma 16.** *H' is a $\mathbb{Z}[x]$-module with the scalar multiplication $\sum_{i=0}^d a_i x^i \cdot \bar{f} \mapsto \prod_{i=0}^d \rho^i(\bar{f})^{a_i}$.*

Our first step for proving Proposition 15 is to show that every element of $G^{\omega,n}$ satisfies a polynomial-order recurrence, modulo some element in $[G^{\omega,n}, G^{\omega,n}]$.

▶ **Lemma 17.** *For every $f \in G^{\omega,n}$, we have $\rho^d(f) \in \langle f\rangle^{(d-1)}[G^{\omega,n}, G^{\omega,n}]$ for $d = n(n+1)/2$.*

Proof. Suppose $f = f_1 \cdots f_m$ such that $f_1, \dots, f_m \in G^\omega$ are elements of period $\le n$. According to Lemma 16, we consider $G^{\omega,n}/[G^{\omega,n}, G^{\omega,n}]$ as a $\mathbb{Z}[x]$-module.

If $g \in G^\omega$ has period q then $\rho^q(g)g^{-1} = 1$ and thus $(x^q - 1)\bar{g} = \rho^q(\bar{g})\bar{g}^{-1} = 1$. Define the polynomial $p(x) = \prod_{i=1}^n (x^i - 1) = \sum_{i=0}^d a_i x^i$ of degree $d = n(n+1)/2$ satisfying $a_d = 1$. Since all functions $f_1, \dots, f_m$ have period at most n, we have $p\bar{f} = 1$. Explicitly, this means $1 = p\bar{f} = \rho^0(\bar{f})^{a_0} \cdot \rho^1(\bar{f})^{a_1} \cdots \rho^d(\bar{f})^{a_d} = \overline{\rho^0(f)^{a_0} \cdots \rho^d(f)^{a_d}}$. Noticing that $a_d = 1$, we can write $\rho^d(f) = gh$ for some $g \in \langle f\rangle^{(d-1)}$ and $h \in [G^{\omega,n}, G^{\omega,n}]$, which has the desired form. ◀

The following lemma gives us control over the remaining factor from $[G^{\omega,n}, G^{\omega,n}]$.

▶ **Lemma 18.** *Let G be a group with nilpotency class c. Then $[G^{\omega,n}, G^{\omega,n}] \subseteq [G,G]^{\omega,n^{2c}}$.*

Proof. We need the fact that the commutator subgroup $[F,F]$ of a group F with generating set Γ is generated by all left-normed commutators $[g_1, \dots, g_k] := [[\dots[[g_1, g_2], g_3], \dots], g_k]$, where $g_1, \dots, g_k \in \Gamma \cup \Gamma^{-1}$ and $k \ge 2$, cf. [6, Lemma 2.6]. Therefore $[G^{\omega,n}, G^{\omega,n}]$ is generated by all left-normed commutators $[g_1, \dots, g_k]$ where $k \ge 2$ and $g_1, \dots, g_k \in G^\omega$ have period at most n. Furthermore, we can bound k by c since any left-normed commutator $[g_1, \dots, g_{c+1}]$ is trivial (recall that G is nilpotent of class c). A left-normed commutator $[g_1, \dots, g_k]$ with $2 \le k \le c$ and $g_1, \dots, g_k$ periodic with period at most n is a product containing at most $2k \le 2c$ distinct functions of period at most n (namely, the $g_1, \dots, g_k$ and their inverses). Hence $[G^{\omega,n}, G^{\omega,n}]$ is generated by functions $g \in [G,G]^\omega$ of period at most n^{2c}. ◀

Proof of Proposition 15. We proceed by induction on the nilpotency class of G. If G has nilpotency class 0, then G is trivial and the claim is vacuous. Now suppose that G has nilpotency class $c \ge 1$. According to Lemma 17, we have $\rho^d(f) \in \langle f\rangle^{(d-1)}h$ for some $h \in [G^{\omega,n}, G^{\omega,n}]$. By Lemma 18, we have $[G^{\omega,n}, G^{\omega,n}] \subseteq [G,G]^{\omega,n^{2c}}$. Since the group $[G,G]$ has nilpotency class at most $c-1$ (we included a proof for this in the full version [9]), we may apply induction. Thus, we know that $\rho^e(h) \in \langle h\rangle^{(e-1)}$ for some $e = e(n^{2c})$. We claim that then $\rho^{d+e}(f) \in \langle f\rangle^{(d+e-1)}$. Note that $\rho^{d+e}(f) \in \rho^e(\langle f\rangle^{(d-1)}h) \subseteq \rho^e(\langle f\rangle^{(d-1)})\rho^e(h) \subseteq \langle f\rangle^{(d+e-1)} \cdot \rho^e(h)$. Therefore, it suffices to show that $\rho^e(h) \in \langle f\rangle^{(d+e-1)}$. Since $\rho^d(f) \in \langle f\rangle^{(d-1)}h$ we have $h \in \langle f\rangle^{(d)}$ and thus $\rho^e(h) \in \langle h\rangle^{(e-1)} \subseteq (\langle f\rangle^{(d)})^{(e-1)} = \langle f\rangle^{(d+e-1)}$. ◀

Proof of Theorem 13. Given periodic functions $f_1, \dots, f_m \in G^\omega$ with maximum period n, and a number $T \in \mathbb{N}$. By Proposition 15 the product $f = f_1 \cdots f_m$ satisfies a recurrence of order d, where d is bounded polynomially in n. Notice that $f = 1$ if and only if $f(t) = 1$ for all $t \le d-1$. Hence, it suffices to verify that $f_1(t) \cdots f_m(t) = 1$ for all $t \le \min\{d, T\}$. This can be accomplished by solving in parallel a polynomial number of instances of the word problem over G, which is contained in TC^0 by [36]. ◀

Proof of Theorem 1. In [27] it is shown that for every f.g. group G, $\textsc{PowerWP}(G \wr \mathbb{Z})$ belongs to $\mathsf{TC}^0(\textsc{Periodic}(G), \textsc{PowerWP}(G))$. By [27] the power word problem for a f.g. nilpotent group belongs to TC^0 and by Theorem 13, $\textsc{Periodic}(G)$ belongs to TC^0. ◀

Proof of Theorem 2. By Theorem 8, $\mathrm{KP}(G \wr \mathbb{Z})$ is NP-hard. For the upper bound we use the following result from [12] that holds for every f.g. group G: There is a non-deterministic polynomial time Turing machine M that takes as input a knapsack expression E over $G \wr \mathbb{Z}$ and outputs in each leaf of the computation tree the following data: (i) an instance of $\textsc{ExpEq}(G)$ and (ii) a finite list of instances of $\textsc{Periodic}(G)$. Moreover, the input expression E has a $(G \wr \mathbb{Z})$-solution if and only if the computation tree has a leaf in which all $\textsc{Periodic}(G)$ instances are positive. If G is finite and nilpotent, then $\textsc{Periodic}(G)$ belongs to TC^0 and $\textsc{ExpEq}(G)$ belongs to NP (this holds for every finite group). The theorem follows. ◀

5 Wreath products with abelian left factors

In this section we consider wreath products $A \wr H$ where A is f.g. abelian and H is a f.g. torsion-free group. We study for which groups H, the complexity of the power word/knapsack problem in H is passed on to $A \wr H$. As applications, we obtain Theorems 3 and 4.

Power word problem over $A \wr H$. As a first step, we *normalize* a given power word $u_1^{k_1} \dots u_d^{k_d}$, i.e. ensure that $u_1, \dots, u_d \in AH$, say $u_i = a_i h_i$ for some $a_i \in A$ and $h_i \in H$ for $1 \le i \le d$. Intuitively, the computation of the power word can be described by finite progressions in the Cayley graph of H, which are labelled with elements a_i from A. The goal is to determine whether the labels on each point cancel out in the abelian group A. Here, a *progression* in H is a sequence $\boldsymbol{p} = (gh^k)_{0 \le k \le \ell}$ with *offset* $g \in H$ and *period* $h \in H$. If $h \ne 1$ then $\boldsymbol{p}$ is a *ray*. For all $1 \le i \le d$ the power word writes the element a_i into the Cayley graph of H along the progression $\boldsymbol{p}_i = (h_1^{k_1} \dots h_{i-1}^{k_{i-1}} h_i^k)_{0 \le k \le k_i}$. Notice that the offset of $\boldsymbol{p}_i$ is given as a power word for $h_1^{k_1} \dots h_{i-1}^{k_{i-1}}$ and the period is given explicitly as a word for the group element h; we call such a progression *power-compressed*.

To solve the power word problem over $A \wr H$ it seems inevitable to compute the intersection set $\{(i,j) \in [0,k] \times [0,\ell] \mid ab^i = gh^j\}$ of two given power-compressed progressions $\boldsymbol{p} = (ab^i)_{0 \le i \le k}, \boldsymbol{q} = (gh^j)_{0 \le j \le \ell}$, for any pair of progressions appearing in the power word. Such a intersection set is always a finite progression in $\mathbb{N}^2$ (c.f. Lemma 9).

However, the key insight of Theorem 3 is that it essentially suffices to compute the intersection of *parallel* rays, i.e. rays with commensurable periods. This is because two non-parallel rays can intersect at most once. Therefore, the number of points in H that cancel to zero with the help of intersections between non-parallel rays can be at most polynomial.

Therefore, roughly speaking, we proceed as follows. Consider a class C of parallel rays from the progressions $\boldsymbol{p}_1, \dots, \boldsymbol{p}_d$. First, we compute the intersection sets of all rays in C. Second, we decide whether the number of points in the support of C which do not cancel to 0 in A exceeds a polynomial bound. In order to count such non-cancelling points, we use Lemma 14 to limit the search to (polynomially many) polynomial-length rays. If our bound on such non-cancelling points is exceeded, then we can reject the entire power word: As mentioned above, non-parallel rays $\boldsymbol{p}_i$ can only intersect at a polynomial number of points in C. If, however, our bound is obeyed, we can explicitly compute the non-cancelling points (as power compressed words) for each parallelity class C and verify that they do evaluate to 0 in the entire set of progressions $\boldsymbol{p}_i$.

In order to (i) compute the intersection set of two parallel power-compressed rays and (ii) count non-cancelling points, we need to solve a generalization of the power word problem in the group H, which we explain next. For a f.g. group $G = \langle \Sigma \rangle$ we define the *power compressed power problem* $\text{PowerPP}(G)$:

Input A word $u \in \Sigma^*$ and a power word $(v_1, k_1, \dots, v_d, k_d)$ over Σ.

Output A binary encoded number $z \in \mathbb{Z}$ with $u^z = v$ where $v = v_1^{k_1} \dots v_d^{k_d}$, or **no** if $u^z = v$ has no solution.

Note that the word u in the input of PowerPP is uncompressed. In order to guarantee that we have small uncompressed inputs to PowerPP, we need to show another property of our groups. Specifically, we prove that the intersection set of parallel rays has a small period: A group $G = \langle \Sigma \rangle$ is *tame with respect to commensurability*, or short *c-tame*, if there exists a number $d \in \mathbb{N}$ such that for all commensurable elements $g, h \in G$ having infinite order there exist numbers $s, t \in \mathbb{Z} \setminus \{0\}$ such that $g^s = h^t$ and $|s|, |t| \le \mathcal{O}((|g| + |h|)^d)$.

Our algorithm for the power word problem sketched above yields the following:

▶ **Proposition 19.** *If the group H is c-tame and torsion-free then $\text{PowerWP}(A \wr H)$ is TC^0-reducible to $\text{PowerPP}(H)$.*

This means, in order to solve the power word problem for groups $W_{m,r}$ and $S_{m,r}$ in TC^0, we also need to solve the power compressed power problem in TC^0. To this end, we first establish TC^0 membership of PowerPP in groups $W_{m,r}$ in the following transfer result.

▶ **Theorem 20.** *Let H and A be f.g. groups where A is abelian and H is c-tame and torsion-free. Then $\text{PowerPP}(A \wr H)$ is TC^0-reducible to $\text{PowerPP}(H)$.*

To show Theorem 20, we provide an elementary (but still somewhat involved) TC^0-reduction from $\text{PowerPP}(A \wr H)$ to $\text{PowerWP}(A \wr H)$ and $\text{PowerPP}(H)$ and apply Proposition 19.

Finally, we need to show that all the groups $W_{m,r}$ and $S_{m,r}$ are c-tame.

▶ **Proposition 21.** *For all $r \ge 1$, $m \ge 0$ the groups $W_{m,r}$ and $S_{m,r}$ are c-tame.*

For Proposition 21, we use elementary arguments and the unique roots property of $W_{m,r}$. The preceding ingredients now yield Theorem 3.

Proof of Theorem 3. We will prove by induction on $m \in \mathbb{N}$ that $\text{PowerPP}(W_{m,r})$ and hence also $\text{PowerWP}(W_{m,r})$ belongs to TC^0. If $m = 0$ then $\text{PowerPP}(W_{0,r})$ is the problem of solving a system of r linear equations $a_i x = b_i$ where a_i is given in unary encoding and b_i is given in binary encoding for $1 \le i \le r$. Since integer division belongs to TC^0 (here, we only have to divide by the unary encoded integers a_i) this problem can be solved in TC^0. The inductive step follows from Theorem 20 and the fact that all groups $W_{m,r}$ are c-tame (Proposition 21) and torsion-free. ◀

Knapsack problem over $A \wr H$. For the knapsack problem we prove the following transfer theorem (recall the definition of an orderable group from Section 3 and the definition of the function $\mathsf{E}_G(n)$ from (2) in Section 3.3):

▶ **Theorem 22.** *Let H and A be f.g. groups where A is abelian and H is orderable and knapsack-semilinear. If $\mathsf{E}_H(n)$ is exponentially bounded then so is $\mathsf{E}_{A \wr H}(n)$.*

The proof of Theorem 22 follows a similar pattern as Theorem 20. The condition that H is orderable ensures that parallel rays in H are contained in cosets of a common cyclic subgroup. We describe the solution set of an exponent equation over $A \wr H$ as a disjunction of polynomially large existential Presburger formulas, which use exponent equations over H and inequalities as atomic formulas. Here, we do not need to algorithmically construct the formula: Its mere existence yields an exponential bound on the size of a solution.

Using Theorem 3 and 22 we can prove Theorem 4: let us fix an iterated wreath product $W = W_{m,r}$ for some $m \geq 0$, $r \geq 1$ (recall that $W_{0,r} = \mathbb{Z}^r$ and $W_{m+1,r} = \mathbb{Z}^r \wr W_{m,r}$). Since $\mathbb{Z}^m$ is orderable, Theorem 7 implies that W is orderable. Moreover, by Theorem 10, W is also knapsack-semilinear. Since by Lemma 11, $\mathsf{E}_A(n)$ is exponentially bounded for every f.g. abelian group A, it follows from Theorem 22 that $\mathsf{E}_W(n)$ is exponentially bounded as well. By Theorem 3 and Lemma 12, $\textsc{ExpEq}(W)$ belongs to NP. Finally, NP-hardness of $\textsc{ExpEq}(W)$ follows from the fact that the question whether a given system of linear Diophantine equations with unary encoded numbers has a solution in $\mathbb{N}$ is NP-hard.

6 Wreath products with difficult knapsack and power word problems

In this section we provide additional details concerning Theorems 5 and 6. We start with a formal definition of uniformly SENS groups [3].

Strongly efficiently non-solvable groups. Let us fix a f.g. group $G = \langle \Sigma \rangle$. Following [3] we need the additional assumption that the generating set Σ contains the group identity 1. This allows to pad words over Σ to any larger length without changing the group element represented by the word. One also says that Σ is a *standard generating set* for G. The group G is called *strongly efficiently non-solvable (SENS)* if there is a constant $\mu \in \mathbb{N}$ such that for every $d \in \mathbb{N}$ and $v \in \{0,1\}^{\leq d}$ there is a word $w_{d,v} \in \Sigma^*$ with the following properties:

- $|w_{d,v}| = 2^{\mu d}$ for all $v \in \{0,1\}^d$,
- $w_{d,v} = [w_{d,v0}, w_{d,v1}]$ for all $v \in \{0,1\}^{<d}$ (here we take the commutator of words),
- $w_{d,\varepsilon} \neq 1$ in G.

The group G is called *uniformly strongly efficiently non-solvable* if, moreover,

- given $v \in \{0,1\}^d$, a binary number i with μd bits, and $a \in \Sigma$ one can decide in linear time on a random access Turing-machine whether the i-th letter of $w_{d,v}$ is a.

In [3] the authors defines also the weaker condition of being (uniformly) efficiently non-solvable. The definition is more technical and it is not clear whether it really leads to a larger class of groups. Examples for uniformly SENS groups are: finite non-solvable groups (more generally, every f.g. group that has a finite non-solvable quotient), f.g. non-abelian free groups, Thompson's group F, and weakly branched self-similar groups with a f.g. branching subgroup (this includes several famous self-similar groups like the Grigorchuk group, the Gupta-Sidki groups and the Tower of Hanoi groups); see [3] for details.

Wreath products with difficult knapsack problems. Recall that Theorem 6 states that $\mathrm{KP}(G \wr \mathbb{Z})$ is Σ_2^p-hard for every uniformly SENS group G. For the proof we consider G-programs. A *G-program* is a sequence of instructions (X, a, b) where X is a boolean variable and a, b are generators of G. Given an assignment for the boolean variables, one can evaluate the G-program in the natural way: If X is set to 1 (resp., 0) then the instruction (X, a, b) evaluates to a (resp. b). The resulting sequence of group generators evaluates to an element of G and this is the evaluation of the G-program under the given assignment. We consider now the following computational problem $\exists\forall$-$\textsc{Sat}(G)$: Given a G-program P, whose variables are split into two sets $\overline{X}$ and $\overline{Y}$, does there exist an assignment $\alpha : \overline{X} \to \{0,1\}$ such that for every assignment $\beta : \overline{Y} \to \{0,1\}$ the program P evaluates to the group identity under the combined assignment $\alpha \cup \beta$?

We prove Theorem 6 in two steps. The first is Σ_2^p-hardness of $\exists\forall$-$\textsc{Sat}(G)$.

▶ **Lemma 23.** *Let the f.g. group $G = \langle \Sigma \rangle$ be uniformly SENS. Then, $\exists\forall$-$\textsc{Sat}(G)$ is Σ_2^p-hard.*

Proof. We prove the lemma by a reduction from the following Σ_2^p-complete problem: given a boolean formula $F = F(\overline{X}, \overline{Y})$ in disjunctive normal form, where $\overline{X}$ and $\overline{Y}$ are disjoint tuples of boolean variables, does the quantified boolean formula $\exists\overline{X}\forall\overline{Y} : F$ hold? Let us fix such a formula $F(\overline{X}, \overline{Y})$. We can write F as a fan-in two boolean circuit of depth $\mathcal{O}(\log|F|)$. By [3, Remark 34] we can compute in logspace from F a G-program P over the variables $\overline{X} \cup \overline{Y}$ of length polynomial in $|F|$ such that for every assignment $\gamma : \overline{X} \cup \overline{Y} \to \{0,1\}$ the following two statements are equivalent:

- $F(\gamma(\overline{X}), \gamma(\overline{Y}))$ holds.
- $P(\gamma) = 1$ in G.

Hence, $\exists\overline{X}\forall\overline{Y} : F$ holds if and only if $\exists\overline{X}\forall\overline{Y} : P = 1$ holds. ◀

The second step is to reduce $\exists\forall$-Sat(G) to $\mathrm{KP}(G \wr \mathbb{Z})$. In fact, this reduction works for any f.g. group G.

▶ **Lemma 24.** *For every f.g. nontrivial group G, $\exists\forall$-Sat(G) is logspace many-one reducible to $\mathrm{KP}(G \wr \mathbb{Z})$.*

Proof sketch. Let us fix a G-program

$$P = (Z_1, a_1, b_1)(Z_2, a_2, b_2) \cdots (Z_\ell, a_\ell, b_\ell) \in ((\overline{X} \cup \overline{Y}) \times \Sigma \times \Sigma)^*$$

where $\overline{X}$ and $\overline{Y}$ are disjoint sets of variables. Let $m = |\overline{X}|$ and $n = |\overline{Y}|$. We want to construct a knapsack expression E over $G \wr \mathbb{Z}$ which has a solution if and only if there is an assignment $\alpha : \overline{X} \to \{0,1\}$ such that $P(\alpha \cup \beta) = 1$ for every assignment $\beta : \overline{Y} \to \{0,1\}$. Let us choose a generator t for $\mathbb{Z}$. Then $\Sigma \cup \{t, t^{-1}\}$ generates the wreath product $G \wr \mathbb{Z}$. First, we compute in logspace the $m+n$ first primes $p_1, \dots, p_{m+n}$ and fix a bijection $p : \overline{X} \cup \overline{Y} \to \{p_1, \dots, p_{m+n}\}$. Moreover, let $M = \prod_{i=1}^{m+n} p_i$.

Roughly speaking, the idea is as follows. Each assignment $\alpha : \overline{X} \to \{0,1\}$ will correspond to a valuation ν for our expression E. The resulting element $\nu(E) \in G \wr \mathbb{Z}$ then encodes the value $P(\alpha \cup \beta)$ for each $\beta : \overline{Y} \to \{0,1\}$ in some position $s \in [0, M-1]$. To be precise, to each $s \in [0, M-1]$, we associate the assignment $\beta_s : \overline{Y} \to \{0,1\}$ where $\beta_s(Y) = 1$ if and only if $s \equiv 0 \bmod p(Y)$. Then, $\tau(\nu(E))(s)$ will be $P(\alpha \cup \beta_s)$. This means, $\nu(E) = 1$ implies that $P(\alpha \cup \beta) = 1$ for all assignments $\beta : \overline{Y} \to \{0,1\}$.

Our expression implements this as follows. For each $i = 1, \dots, \ell$, it walks to the right to some position $M' \geq M$ and then walks back to the origin. On the way to the right, the behavior depends on whether Z_i is an existential or a universal variable. If Z_i is existential, we either place a_i at every position (if $\alpha(Z_i) = 1$) or b_i at every position (if $\alpha(Z_i) = 0$). If Z_i is universal, we place a_i in the positions divisible by $p(Z_i)$; and we place b_i in the others. That way, in position $s \in [0, M-1]$, the accumulated element will be $P(\alpha \cup \beta_s)$. The complete proof can be found in the full version [9]. ◀

Let us now show some applications of Theorem 6:

▶ **Corollary 25.** $\mathrm{KP}(G \wr \mathbb{Z})$ *is Σ_2^p-complete for G finite non-solvable or f.g.non-abelian free.*

Proof. Finite non-solvable groups and f.g. non-abelian free groups are uniformly SENS [3]. By Theorem 6, $\mathrm{KP}(G \wr \mathbb{Z})$ is Σ_2^p-hard. It remains to show that $\mathrm{KP}(G \wr \mathbb{Z})$ belongs to Σ_2^p. According to [12] (see also the proof of Theorem 2) it suffices to show that Periodic(G) and ExpEq(G) both belong to Σ_2^p. The problem Periodic(G) belongs to coNP (since the word problem for G can be solved in polynomial time) and ExpEq(G) belongs to NP. For a finite group this is clear and for a free group one can use [29]. ◀

Theorem 6 can be also applied to Thompson's group F. This is one of the most well studied groups in (infinite) group theory due to its unusual properties, see e.g. [5]. It can be defined in several ways; let us just mention the following finite presentation: $F = \langle x_0, x_1 \mid [x_0x_1^{-1}, x_0^{-1}x_1x_0], [x_0x_1^{-1}, x_0^{-2}x_1x_0^2]\rangle$. Thompson's group F is uniformly SENS [3] and contains a copy of $F \wr \mathbb{Z}$ [14]. Theorem 6 yields:

▶ **Corollary 26.** *The knapsack problem for Thompson's group F is Σ_2^p-hard.*

We conjecture Σ_2^p-completeness. Since F is co-context-free [23], $\mathrm{KP}(F)$ is decidable [22].

Wreath product with difficult power word problems. In [27] it was shown that the problem $\textsc{PowerWP}(G \wr \mathbb{Z})$ is coNP-complete in case G is a finite non-solvable group or a f.g. free group. The proof in [27] immediately generalizes to the case were G is uniformly SENS. This yields Theorem 5. Alternatively, one can prove Theorem 5 by showing that

- $\forall$-$\textsc{Sat}(G)$ (the question whether a given G-program P evaluates to the group identity for all assignment) is coNP-hard if G is uniformly SENS, and
- $\forall$-$\textsc{Sat}(G)$ is logspace many-one reducible to $\textsc{PowerWP}(G \wr \mathbb{Z})$.

This can be shown with the same reductions as in Lemmas 23 and 24.

Fix a f.g. group $G = \langle\Sigma\rangle$. With $\mathrm{WP}(G, \Sigma)$ we denote the set of all words $w \in \Sigma^*$ such that $w = 1$ in G (the word problem for G with respect to Σ). We say that G is *co-context-free* if $\Sigma^* \setminus \mathrm{WP}(G, \Sigma)$ is context-free (the choice of Σ is not relevant for this) [18, Section 14.2].

▶ **Theorem 27.** *The power word problem for a co-context-free group G belongs to* coNP.

Proof. The following argument is similar to the decidability proof for knapsack in co-context-free groups in [22]. Let $G = \langle\Sigma\rangle$ and let $(u_1, k_1, u_2, k_2, \ldots, u_d, k_d)$ be the input power word, where $u_i \in \Sigma^*$. We can assume that all k_i are positive. We have to check whether $u_1^{k_1}u_2^{k_2}\cdots u_d^{k_d}$ is trivial in G. Let L be the complement of $\mathrm{WP}(G, \Sigma)$, which is context-free. Take the alphabet $\{a_1, \ldots, a_d\}$ and define the morphism $h : \{a_1, \ldots, a_d\}^* \to \Sigma^*$ by $h(a_i) = u_i$. Consider the language $K = h^{-1}(L) \cap a_1^* a_2^* \cdots a_d^*$. Since the context-free languages are closed under inverse morphisms and intersections with regular languages, K is context-free too. Moreover, from the tuple $(u_1, u_2, \ldots, u_d)$ we can compute in polynomial time a context-free grammar for K: Start with a push-down automaton M for L (since L is a fixed language, this is an object of constant size). From M one can compute in polynomial time a push-down automaton M' for $h^{-1}(L)$: when reading the symbol a_i, M' has to simulate (using ε-transitions) M on $h(a_i)$. Next, we construct in polynomial time a push-down automaton M'' for $h^{-1}(L) \cap a_1^* a_2^* \cdots a_d^*$ using a product construction. Finally, we transform M'' back into a context-free grammar. This is again possible in polynomial time using the standard triple construction. It remains to check whether $a_1^{k_1}a_2^{k_2}\cdots a_d^{k_d} \notin L(G)$. This is equivalent to $(k_1, k_2, \ldots, k_d) \notin \Psi(L(G))$, where $\Psi(L(G))$ denotes the Parikh image of $L(G)$. Checking $(k_1, k_2, \ldots, k_d) \in \Psi(L(G))$ is an instance of the uniform membership problem for commutative context-free languages, which can be solved in NP according to [19]. This implies that the power word problem for G belongs to coNP. ◀

▶ **Theorem 28.** *For Thompson's group F, the power word problem is* coNP*-complete.*

Proof. Since F is co-context-free [23], Theorem 27 yields the upper bound. The lower bound follows from Theorem 5 and the facts that F is uniformly SENS and that $F \wr \mathbb{Z} \leq F$. ◀

7 Open problems

Our results naturally lead to several open research problems:

- Theorems 1 and 5 leave some room for further improvements. In this context, a particularly interesting problem is the power word problem for a wreath product $G \wr \mathbb{Z}$, where G is finite solvable but not nilpotent. Recall that for Theorem 5 we reduced $\forall$-SAT(G) to POWERWP($G \wr \mathbb{Z}$). This reduction works for every non-trivial f.g. group. Moreover, the problem whether a given equation $u = v$ with variables holds in G for all assignments of the variables to elements of G (called EQNID(G) in [44]) can be easily reduced to $\forall$-SAT(G). This allows us to apply recent results from [44], where the author constructs finite solvable groups G for which EQNID(G) cannot be solved in polynomial time assuming the exponential time hypothesis (this holds for instance for all finite solvable groups of Fitting length at least 4). Hence, there is no hope to find a polynomial time algorithm for the power word problem for $G \wr \mathbb{Z}$ for every finite solvable group G, but one can still look at restricted classes of solvable groups.
- We believe that in Theorem 22, the assumption that H is orderable is not needed. In other words, we conjecture the following: Let H and A be f.g. groups where A is abelian and H is knapsack-semilinear. If $\mathsf{E}_H(n)$ is exponentially bounded then so is $\mathsf{E}_{A \wr H}(n)$.
- Recall the we proved that knapsack for Thompson's group F is Σ_2^p-hard. Decidability of knapsack for Thompson's group F follows from [22] and the fact that F is co-context-free. It is shown in [22] that for every co-context-free group the knapsack problem reduces to checking non-universality of the Parikh image of a bounded context-free language. The latter problem belongs to NEXPTIME [20, Theorem 2.10] (see also [16, Corollary 1]). It would be interesting to find better complexity bounds for this problem.

References

1 Lazlo Babai, Robert Beals, Jin-Yi Cai, Gábor Ivanyos, and Eugene M. Luks. Multiplicative equations over commuting matrices. In *Proceedings of SODA 1996*, pages 498–507. ACM/SIAM, 1996.

2 David A. Mix Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1. *Journal of Computer and System Sciences*, 38:150–164, 1989.

3 Laurent Bartholdi, Michael Figelius, Markus Lohrey, and Armin Weiß. Groups with ALOGTIME-hard word problems and PSPACE-complete compressed word problems. Technical report, arXiv.org, 2020. https://arxiv.org/abs/1909.13781.

4 William Boone. The word problem. *Annals of Mathematics. Second Series*, 70:207–265, 1959.

5 John W. Cannon, William J. Floyd, and Walter R. Parry. Introductory notes on Richard Thompson's groups. *L'Enseignement Mathématique*, 42(3):215–256, 1996.

6 Anthony E. Clement, Stephen Majewicz, and Marcos Zyman. *The Theory of Nilpotent Groups*. Springer, 2017.

7 Max Dehn. Über unendliche diskontinuierliche Gruppen. *Mathematische Annalen*, 71:116–144, 1911. In German.

8 Michael Elberfeld, Andreas Jakoby, and Till Tantau. Algorithmic meta theorems for circuit classes of constant and logarithmic depth. *Electronic Colloquium on Computational Complexity (ECCC)*, 18:128, 2011.

9 Michael Figelius, Moses Ganardi, Markus Lohrey, and Georg Zetzsche. The complexity of knapsack problems in wreath products. *CoRR*, abs/2002.08086, 2020. URL: https://arxiv.org/abs/2002.08086.

10 Michael Figelius, Markus Lohrey, and Georg Zetzsche. Closure properties of knapsack semilinear groups. *CoRR*, abs/1911.12857, 2019. URL: https://arxiv.org/abs/1911.12857.

11 Elizaveta Frenkel, Andrey Nikolaev, and Alexander Ushakov. Knapsack problems in products of groups. *Journal of Symbolic Computation*, 74:96–108, 2016.

12 Moses Ganardi, Daniel König, Markus Lohrey, and Georg Zetzsche. Knapsack problems for wreath products. In *Proceedings of STACS 2018*, volume 96 of *LIPIcs*, pages 32:1–32:13. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018.

13 Guoqiang Ge. Testing equalities of multiplicative representations in polynomial time (extended abstract). In *Proceedings of the 34th Annual Symposium on Foundations of Computer Science, FOCS 1993*, pages 422–426. IEEE Computer Society, 1993.

14 Victor S. Guba and Mark V. Sapir. On subgroups of the R. Thompson group F and other diagram groups. *Mat. Sb.*, 190(8):3–60, 1999.

15 Christoph Haase. *On the complexity of model checking counter automata*. PhD thesis, University of Oxford, St Catherine's College, 2011.

16 Christoph Haase. Subclasses of Presburger arithmetic and the weak EXP hierarchy. In *Proceedings of CSL-LICS 2014*, pages 47:1–47:10. ACM, 2014.

17 Tore Herlestam. On functions of linear shift register sequences. In *Proceedings of EUROCRYPT '85*, volume 219 of *Lecture Notes in Computer Science*, pages 119–129. Springer, 1986.

18 Derek F. Holt, Sarah Rees, and Claas E. Röver. *Groups, Languages and Automata*, volume 88 of *London Mathematical Society Student Texts*. Cambridge University Press, 2017.

19 Dung T. Huynh. Commutative grammars: The complexity of uniform word problems. *Information and Control*, 57:21–39, 1983.

20 Dung T. Huynh. The complexity of equivalence problems for commutative grammars. *Information and Control*, 66(1/2):103–121, 1985.

21 Richard M. Karp. Reducibility among combinatorial problems. In R. E. Miller and J. W. Thatcher, editors, *Complexity of Computer Computations*, pages 85–103. Plenum Press, 1972.

22 Daniel König, Markus Lohrey, and Georg Zetzsche. Knapsack and subset sum problems in nilpotent, polycyclic, and co-context-free groups. In *Algebra and Computer Science*, volume 677 of *Contemporary Mathematics*, pages 138–153. American Mathematical Society, 2016.

23 Jörg Lehnert and Pascal Schweitzer. The co-word problem for the Higman-Thompson group is context-free. *Bulletin of the London Mathematical Society*, 39(2):235–241, 2007.

24 Markus Lohrey. *The Compressed Word Problem for Groups*. SpringerBriefs in Mathematics. Springer, 2014.

25 Markus Lohrey. Knapsack in hyperbolic groups. *Journal of Algebra*, 545:390–415, 2020.

26 Markus Lohrey, Benjamin Steinberg, and Georg Zetzsche. Rational subsets and submonoids of wreath products. *Information and Computation*, 243:191–204, 2015.

27 Markus Lohrey and Armin Weiß. The power word problem. In *Proceedings of MFCS 2019*, volume 138 of *LIPIcs*, pages 43:1–43:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

28 Markus Lohrey and Georg Zetzsche. Knapsack in graph groups, HNN-extensions and amalgamated products. In *Proceedings of STACS 2016*, volume 47 of *LIPIcs*, pages 50:1–50:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016.

29 Markus Lohrey and Georg Zetzsche. Knapsack in graph groups. *Theory of Computing Systems*, 62(1):192–246, 2018.

30 Patrizia Longobardi and Mercede Maj. On some classes of orderable groups. *Milan Journal of Mathematics*, 68(1):203–216, 1998.

31 R. C. Lyndon and Paul E. Schupp. *Combinatorial Group Theory*. Springer, 1977.

32 Wilhelm Magnus. On a theorem of Marshall Hall. *Annals of Mathematics. Second Series*, 40:764–768, 1939.

33 Alexei Miasnikov, Andrey Nikolaev, and Alexander Ushakov. Knapsack problems in groups. *Mathematics of Computation*, 84:987–1016, 2015.

34 Alexei Miasnikov, Vitaly Roman'kov, Alexander Ushakov, and Anatoly Vershik. The word and geodesic problems in free solvable groups. *Transactions of the American Mathematical Society*, 362(9):4655–4682, 2010.

35 Alexei Miasnikov, Svetla Vassileva, and Armin Weiß. The conjugacy problem in free solvable groups and wreath products of abelian groups is in TC^0. *Theory of Computing Systems*, 63(4):809–832, 2019.

36 Alexei Miasnikov and Armin Weiß. TC^0 circuits for algorithmic problems in nilpotent groups. In *Proceedings of MFCS 2017*, volume 83 of *LIPIcs*, pages 23:1–23:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017.

37 Alexei Mishchenko and Alexander Treier. Knapsack problem for nilpotent groups. *Groups Complexity Cryptology*, 9(1):87–98, 2017.

38 Roberta Mura and Akbar H. Rhemtulla. *Orderable groups*. Marcel Dekker, 1977.

39 Bernhard Hermann Neumann. On ordered groups. *American Journal of Mathematics*, 71(1):1–18, 1949.

40 Pyotr S. Novikov. On the algorithmic unsolvability of the word problem in group theory. *American Mathematical Society, Translations, II. Series*, 9:1–122, 1958.

41 Dale Rolfsen. Low-dimensional topology and ordering groups. *Mathematica Slovaca*, 64(3):579–600, 2014.

42 Heribert Vollmer. *Introduction to Circuit Complexity*. Springer, 1999.

43 Joachim von zur Gathen and Malte Sieveking. A bound on solutions of linear integer equalities and inequalities. *Proceedings of the American Mathematical Society*, 72(1):155–158, 1978.

44 Armin Weiß. Hardness of equations over finite solvable groups under the exponential time hypothesis. *CoRR*, abs/2002.10145, 2020. URL: `https://arxiv.org/abs/2002.10145`.